

SLIP SLIDING AWAY

By David Whelan
The Law Society of Upper Canada

The allure of mobility calls out to all lawyers. But while we enjoy the opportunity to compute remotely, do not forget a potential downside: the vulnerability of client and law firm data.

Even the smartest lawyer can get flustered at a crowded TSA checkpoint, or jostled in a Manhattan taxi. Mobile devices are small and lightweight, which is great — but small and light also means they can drop out of pockets or slide from purses. And small and light also makes them easy prey for nimble pickpockets.

So what happens if you lose control of your device and it has critical, confidential data on it? Worst case scenario, you could jeopardize a client's case, lose your job, or give an identity thief a jackpot and spend months repairing your credit. None are risks worth taking.

ENCRYPTION

The good news is one single word: encryption. Laptop users have the most encryption options, but some products also can be used to secure USB drives, smartphones, and PDAs. You can encrypt either your entire computer or some of the files on it.

If you aren't yet comfortable with "whole disk" encryption, you can bite off your data security challenge in smaller pieces.

Your operating system's data encryption may limit you to file system-level encryption. If you use Microsoft Corp.'s Windows 2000, XP, or most Vista operating systems, you have the encrypting file system (EFS), although it is limited to non-system files and folders.

Similarly, Apple Inc. users of FileVault (www.apple.com) can only encrypt their home folder on their primary drive. When you are logged in, your EFS or FileVault encrypted files are accessible to you and to anyone with whom you have shared them.

So you may want to turn to third-party software, such as PGP Corp.'s PGP Desktop Professional and TrueCrypt Foundation's namesake open source product, that enhance file system-level encryption. For example, you can create a TrueCrypt "volume" that looks like a single file on your hard drive. When you "mount" it, it appears as a virtual disk drive which you can use like any other storage drive.

You can even redirect your Windows' My Documents folder to a mounted encrypted volume, reducing the chances you will save information in an unencrypted folder. When you walk away from your computer, just dismount the volume, and your encrypted information is no longer accessible even though you are still logged in to your computer.

File system-level encryption can alleviate one common fear: what if I forget my decryption password and lose it all! It lets you reduce the number of files that could potentially be lost. When you back up your files to your firm network, you can minimize this risk further. However, file system-level encryption can be more time consuming — mounting and dismounting volumes, for example — and may still not encrypt everything on your portable device. Unless you are encrypting web cache, temporary folders, and other data locations, you may find that some data you thought was encrypted isn't.

On the other hand, whole disk encryption will ensure that everything on your disk remains inaccessible if your laptop is stolen. A password is required to start up the computer, and without it, even if the hard drive is removed and placed in another machine, the data remains inaccessible.

The flip side is that you must "remember that you should use encryption in an environment where you accept that the 'live' data to be encrypted may be lost," according to Microsoft Vista for IT Security Professionals (<http://tinyurl.com/MSVistaforITProsGB>). Without the password to unlock the encryption software, you have no better access to your information than anyone else.

Microsoft's Vista Enterprise and Vista Ultimate operating systems have Bitlocker built in, providing whole disk encryption. A slew of third-party products also have moved into the whole disk market, focusing on "endpoint" security.

Major PC security firms have incorporated smaller encryption applications — Safeboot by McAfee Inc. (www.dataprotection.mcafee.com); Pointsec by Checkpoint (www.checkpoint.com); GuardianEdge Inc.'s (www.guardianedge.com) OEM deal with Symantec Corp. (www.symantec.com) — to provide mid-size and large organization encryption options. These are designed to secure any "endpoint" — e.g., PC, PDA, smartphone with data — on the organization's network. Products such as PGP's Whole Disk and TrueCrypt also offer options for whole disk encryption, and PGP has a number of encryption products for large organizations.

Whole disk encryption offers a number of benefits. A single password unlocks the entire device, so that you don't need to remember to mount or dismount encrypted volumes, or worry that you have left part of your disk unencrypted.

It's not completely bulletproof, however, as shown in a 2008 paper by Princeton researchers (<http://citp.princeton.edu/pub/coldboot.pdf>, or <http://citp.princeton.edu/memory>).

They retrieved encryption keys from the memory of laptops left in standby and hibernation mode, and accessed encrypted files despite use of whole disk encryption.

Just as you should be sure that you are backing up your data before you hit the road, make sure to power off your laptop when it is not in use. If it's stolen but turned off, you can eliminate this security hole.

If you are carrying sensitive data with you, whether it's privileged client information or just information you'd rather keep private, encrypting your mobile device has never been easier. You can also encrypt your desktop PC data with these products. Options are available for solo lawyers up to large firm enterprise installations. For your own piece of mind if nothing else, protect your practice by encrypting your data.

***David Whelan** is a long-time member of Law Technology News' Editorial Advisory Board. He is manager, legal information and corporate records and archives, for the Law Society of Upper Canada. Whelan is based in Toronto, Canada. E-mail: dwhelan@lsuc.on.ca.*

Reprinted with permission from the November 2008 edition of Law Technology News. (c) 2008 ALM Properties, Inc., an Incisive Media Company. All rights reserved. Further duplication without permission is prohibited.